REMARKS

Claim Rejections Section 102(e)

Regarding the rejections for anticipation by Casey (US6493349), independent claim 1 has been amended to recite the novel feature that "the VPN gateway providing a plurality of virtual routers, respective ones of said plurality of virtual routers being connected to respective ones of said two or more VPNs such that each virtual router is in the address space of a respective one of said two or more VPNs". Basis for this change is found at page 9, lines 25 to 32 of the specification as filed. Independent claim 13 has been similarly changed, but independent claim 14 has been deleted.

As indicated at page 9, lines 15 to 25, the VPN gateway performs two functions, that of a router and that of a network address translator (NAT) on a common or shared basis for the two or more VPNs. As such, each of the two or more VPNs appears to have a dedicated call server despite its being a shared resource.

Casey neither teaches nor suggests such an arrangement.

The primary purpose of Casey is to fragment a VPN into a plurality of logically contiguous VPN areas based on different IP VPN technologies. As such, Casey discloses a fragmented VPN in which the VPN is separated into areas, each VPN area being implemented by a single IP VPN technology dependent on what technology the network provider (operator) for that VPN area can deliver. For example, in one of the VPN areas, the provider for that area might operate a MPLS based IP VPN whereas in another VPN area the provider for that area might operate an IP over Local Area Network Emulation (LANE) IP VPN. There is no suggestion in Casey that any VPN gateway shared by two or more VPNs incorporates both routing and NAT functionality as claimed. In fact, the arrangement of Casey, even if it does indeed disclose what the Examiner contends, is representative of the prior art arrangement of figure 2 of the present application and presents the same disadvantageous

regarding the need for network translation of addresses between the different addressing schemes of the VPNs and the external networks.

The remaining claims have the same distinctive feature or are dependent on such a claim, and so are acceptable for the same reasons.

That being said, with respect to claim 2, it cannot be said that column 3, lines 27 to 56 and column 4, lines 8 to 56 of Casey teach anything about network address translation. Whilst the virtual routers taught by Casey operate full routing protocols, they do so in respect of controlling routing exchanges relating to the IP address spaces of the private networks. However, a routing regime can be specific to an individual VPN and a virtual router may use different routing protocols on each of its interfaces. None of this, however, amounts to network address translation and, if the Examiner is of the view that it does, he/she is asked to explain how. Furthermore, as taught in paragraph 0039 of Casey, a virtual router applies a forward control process in respect of the private network address space based on the identity of an incoming tunnel and a forwarding table. This also does not amount to network address translation as one skilled in the art would understand this term of art to mean. As is apparent from Boden (U2003/0149899), serious issues arise when attempting network address translation on IP addresses within tunnels – see "Background of the Invention" section of Boden. Consequently, the Examiner must explain why, if Casey teaches the combination of routing and network address translation in the VPN gateway rather than separately as in prior art arrangements (figure 2 of the present application, for example), why such issues as acknowledged by Boden with respect to tunnels do not appear to arise in the case of Casey, given that Casey is concerned with processing tunnels. The reason, of course, that Casey is silent on such issues is that it does not teach address translation within a VPN gateway providing both VPN routing and network address translation functions and thus the issues relating to tunnels do not arise.

In conclusion, Casey does not teach or suggest that any VPN gateway shared by two or more VPNs incorporates both routing and NAT functionality and

certainly does not teach or suggest that a virtual router performs network address translation. If the Examiner remains of the view that it does offer such a teaching, he/she must explain how this is implemented in the presence of the incoming tunnel identity/forwarding table process that is explicitly taught by Casey. Otherwise, claim 1 should be acknowledged as not being anticipated or rendered obvious by Casey.

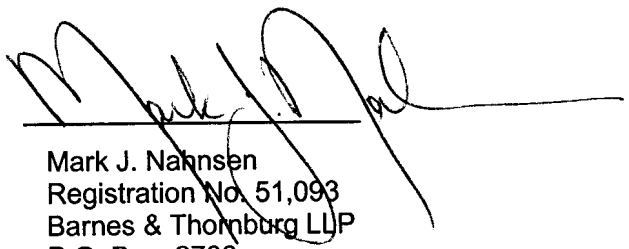
Similar observations can be made in respect of other dependent claims.

Referring now to the Examiner's rejection of claims 1, 13 and 14 as being anticipated by Boden under 35 USC s 102(e), Applicant respectfully disagrees. As is clear from paragraph 0031 of Boden, in order to provide an IPSec gateway incorporating NAT functionality, it is an essential requirement that IPSec connections and thus IPSec processing begins and ends at the IPSec gateway. As such, any virtual routing function provided by the IPSec gateway for a VPN cannot have the same (private) address space of the VPN to which it is connected. Thus, not only does Boden not teach all of the claims limitations, but it teaches that one of the claimed limitations is entirely incompatible with what is taught by Boden. Consequently, the claims as presented herein are not anticipated or rendered obvious by Boden.

All the points raised by the Examiner have now been dealt with and favorable reconsideration is requested.

March 28, 2008

Respectfully submitted,



Mark J. Nahnsen
Registration No. 51,093
Barnes & Thornburg LLP
P.O. Box 2786
Chicago, Illinois 60690-2786
Phone: 312-214-4810
Facsimile: 312-759-5646
E-mail: mnahnsen@btlaw.com